Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018

Date filed: February 20, 2018

Name of company covered by this certification: Hudson Fiber Networks, Inc.

Form 499 Filer ID:	828735
Name of signatory:	Robert Hagan
Title of signatory:	CFO

I, Robert Hagan, certify that I am an officer of Hudson Fiber Networks, Inc. ("Hudson Fiber" or "Company"}, and acting as an agent of Hudson Fiber, that I have personal knowledge that Hudson Fiber has established operating procedures that are adequate to ensure compliance with the commission's CPNI rules. *See* 47 C.F.R. §64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how Hudson Fiber's procedures ensure that the Company is in compliance with the requirements (including, where applicable, those mandating the adoption of CPNI procedures, training, safeguards, record keeping and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

Hudson Fiber has not taken any actions (i.e., proceedings instituted or petitions filed by Hudson Fiber at either state commissions, the court system, or at the Commission) against data brokers in the past year, nor is there any evidence that pretexters attempted to access CPNI maintained by Hudson Fiber.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed
Robert Hagan
CFO
Hudson Fiber Networks, Inc.

HUDSON FIBER NETWORKS, INC. STATEMENT OF COMPLIANCE WITH CPNI RULES

Hudson Fiber Networks, Inc. ("Hudson Fiber" or "Company") is a Private Service Provider providing services to other telecommunications carriers and application service providers that are designed to broaden and enhance their ability to interconnect their respective networks and allow them to exchange traffic with one another more effectively and efficiently. The Company's operations are focused on the provision of tandem switching and transport services to wireless carriers, interexchange carriers, competitive local exchange carriers and incumbent local exchange carriers.

The Company only has access to limited forms of CPNI from its carrier customers and has adopted various operational procedures to assure that, consistent with the Commission's rules, all of the CPNI that it holds is protected from unauthorized and unlawful use, access and disclosure.

Consistent with the CPNI rules, the Company may use, disclose and permit access to CPNI without customer approval (1) to render, bill and collect for services provided; (2) to protect rights or property of the Company, other users or other carriers from unlawful use; (3) for the purpose of network maintenance, repair and troubleshooting; and (4) to comply with a valid legal process such as a subpoena, court order, or search warrant.

The Company does not use, disclose or permit access to CPNI for marketing purposes other than for the purpose of providing service offerings for the type of services to which the Company's customer already subscribes. It is therefore not required to seek approval from existing customers to use their CPNI and does not maintain a record of a customer's approval to use CPNI. In the event the Company changes its marketing practices or expands its service offerings so that customer approval is required, it will implement a system by which customers will be notified of such use and the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Furthermore, the Company does not share, sell, lease or otherwise provide CPNI to any of its affiliates, suppliers, vendors and any other third parties for the purposes of marketing any services.

The Company has effectuated processes and procedures to train its personnel as to when they are and are not permitted to use CPNI and has completed such training and will periodically refresh such training (at minimum, annually). For instance, all Company employees receive CPNI training and are required to abide by the Company's CPNI Protection Policy, which, *inter alia,* requires employees to maintain the confidentiality of all information, including CPNI, which may be obtained as a result of their employment by the Company. The Company's CPNI Protection Policy also provides a comprehensive roadmap of how Company employees are required to use, maintain and disclose CPNI. Employees who violate the Company's CPNI Protection Policy are subject to disciplinary action, ranging from written warnings to possible termination, depending on the nature, frequency, and severity of the violation(s).

To the extent the Company engages in any marketing campaigns, it has established a supervisory review and approval process to ensure that such campaigns are consistent with FCC's CPNI rules. The Company maintains a record for at least one year of its own and, if applicable, affiliates' sales and marketing campaigns, if any, that use customers' CPNI.

The Company does not provide its customers or their customers CPNI without proper customer authentication on inbound telephone calls, in accordance with contractual arrangements. The Company only discusses over the phone callinformation of its customers' end user customers that is provided by the customer. With respect to call detail information pertaining to end users of the Company's customers' services, the Company uses the information in switch records that are generated when the Company provides its tandem and transport services to bill for such services. The information in these switch records is not organized in a manner that would allow the Company to identify any individual end user customers and the Company only shares that information with its customers who are properly authenticated and then only by sending those records to the applicable customer's address of record . All Company customers have dedicated account representatives who serve as the primary customer contact. The account representatives personally know each customer. Currently the Company does not provide in-store account access for its customers.

If a customer's address changes, the Company will notify the customer of that change by mailing such notice to the customer's address of record consistent with the FCC's CPNI rules. In the event of a breach of CPNI that is maintained by the Company, it will provide law enforcement with electronic notice of such CPNI breach as soon as practicable and not later than 7 business days after reasonable determination of the breach. After notifying law enforcement and unless directed otherwise, the Company will notify affected customers not earlier than 7 full business days later and will maintain a record of any CPNI-related breaches and the related notifications for a period of at least 2 years as required by the applicable FCC CPNI rules.

In the event that the Company changes its marketing practices such that opt-out notices are required, the Company will implement procedures whereby it will provide the FCC written notice within 5 business days of any instance where the opt-out mechanisms do not work properly, to such a degree that customers' inability to opt-out is more than an anomaly.